



CyberSecurity, US CNCI-SCRM, Public-Private STANDARDIZATION ...

13th Semi-Annual Software Assurance (SwA) Forum

@

NIST HQS

27 Sep – 1 Oct 2010

Don.Davidson@osd.mil

Trusted Mission Systems & Networks

OASD-NII / DoD CIO



CYBERSECURITY





Comprehensive National Cybersecurity Initiative (CNCI)



Focus Area 1

Trusted Internet Connections

Deploy Passive Sensors Across Federal Systems

Pursue Deployment of Intrusion Prevention System
(Dynamic Defense)

Coordinate and Redirect R&D Efforts

Establish a front line of defense

Focus Area 2

Connect Current Centers to Enhance Cyber Situational Awareness

Develop a Government Wide Cyber Counterintelligence Plan

Increase the Security of the Classified Networks

Expand Education

Demonstrate resolve to secure U.S. cyberspace & set conditions for long-term success

Focus Area 3

Define and Develop Enduring Leap Ahead Technology, Strategies & Programs

Define and Develop Enduring Deterrence Strategies & Programs

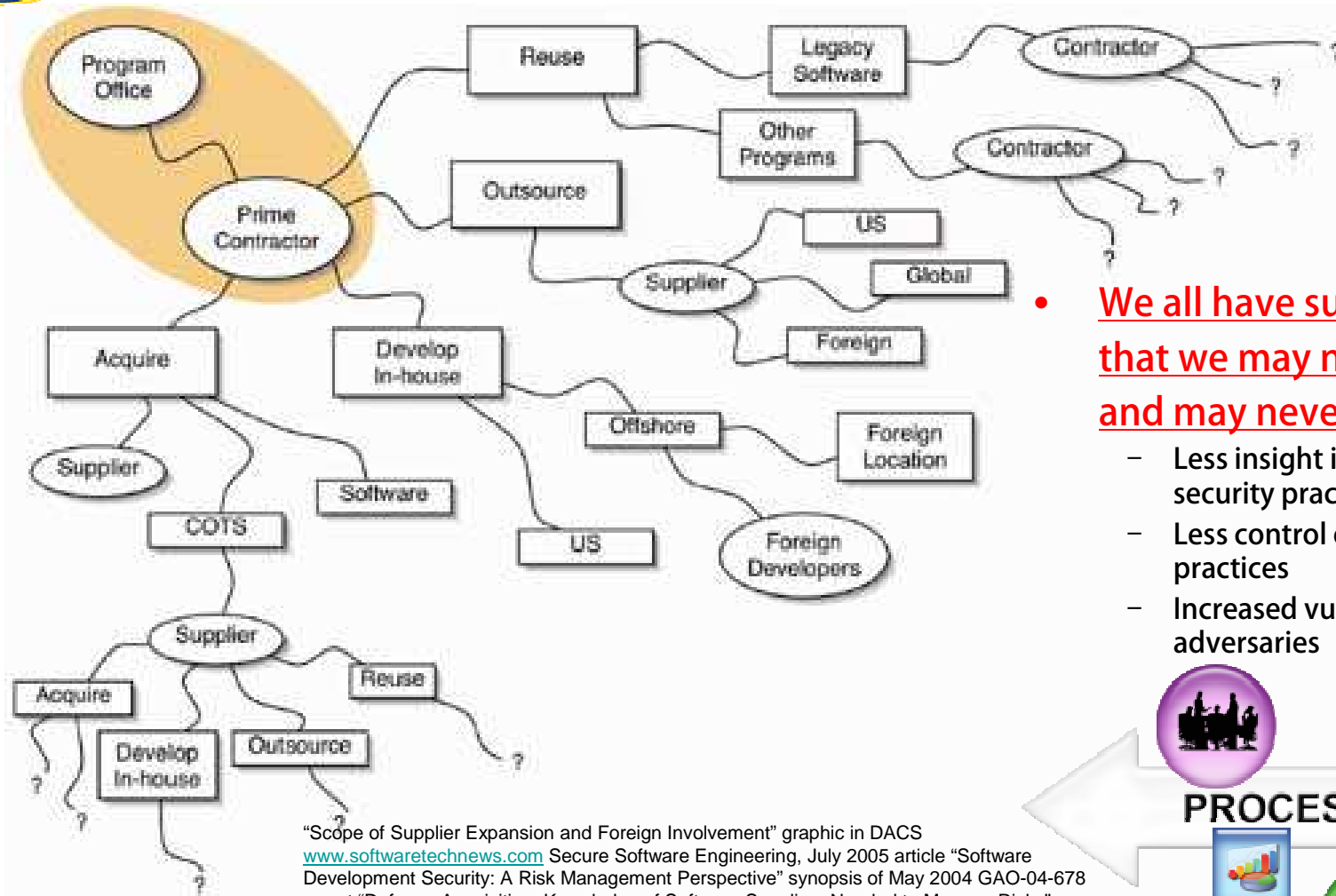
Develop Multi-Pronged Approach for Global Supply Chain Risk Management

Define the Federal Role for Extending Cybersecurity into Critical Infrastructure Domains

Shape the future environment to demonstrate resolve to secure U.S. technological advantage and address new attack and defend vectors



Globalization brings challenges



- We all have suppliers that we may not know and may never see

- Less insight into suppliers' security practices
- Less control over business practices
- Increased vulnerability to adversaries



PROCESS



"Scope of Supplier Expansion and Foreign Involvement" graphic in DACS
www.softwaretechnews.com Secure Software Engineering, July 2005 article "Software Development Security: A Risk Management Perspective" synopsis of May 2004 GAO-04-678 report "Defense Acquisition: Knowledge of Software Suppliers Needed to Manage Risks"



Today's Reality of our Increased Dependency Requires an Increased Confidence in our ICT



- Dependencies on technology are greater than ever
- Possibility of disruption is greater than ever because software (and overall ICT) is vulnerable
- Loss of confidence alone can lead to stakeholder actions that disrupt critical business activities



Internet users in the world: 1,766,727,004
E-mail messages sent today: 215, 674, 475, 422
Blog Posts Today: 458, 972
Google searches Today: 2,302,204,936

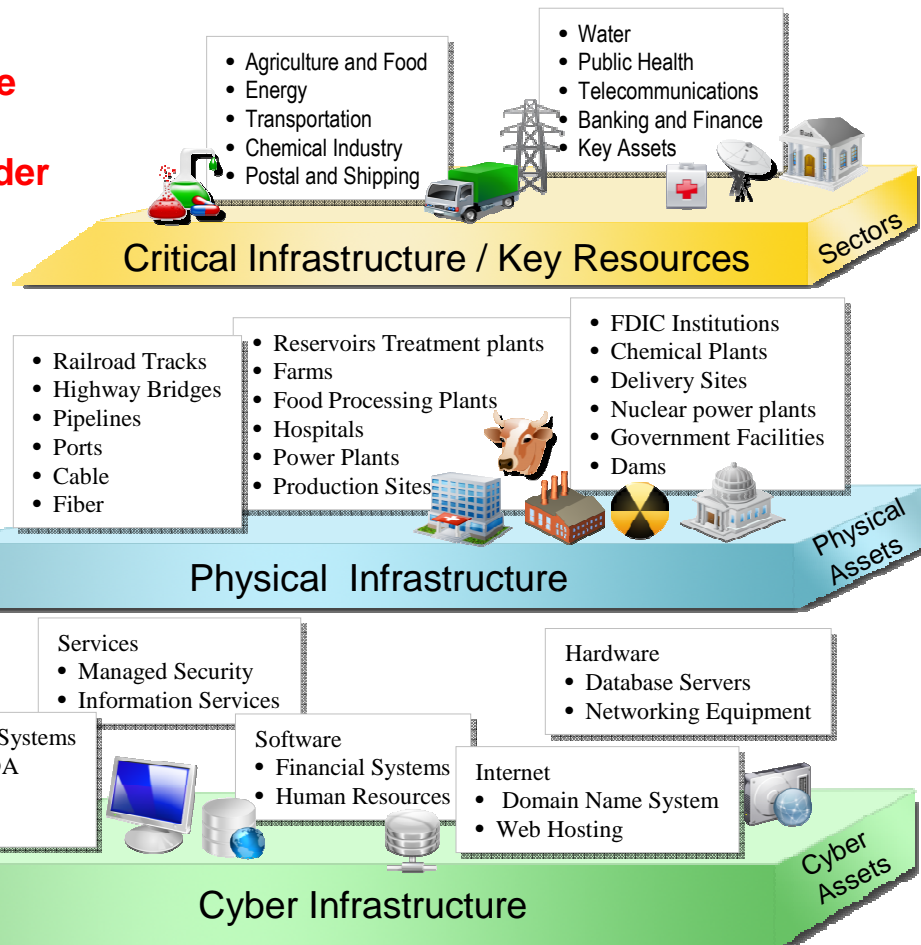
Who is behind data breaches?

74% resulted from external sources (+1%).
20% were caused by insiders (+2%).
32% implicated business partners (-7%).
39% involved multiple parties (+9%).

How do breaches occur?

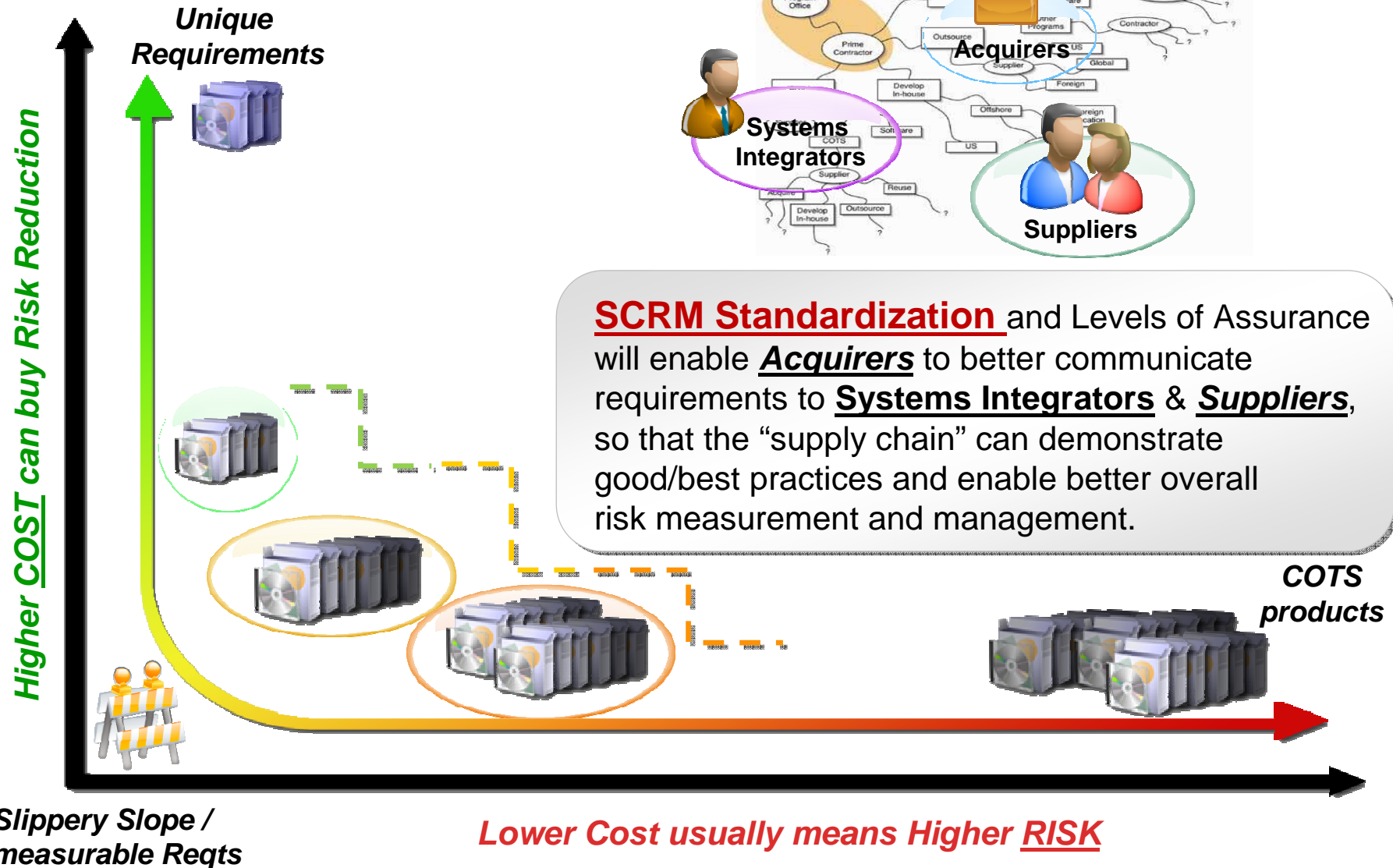
7% were aided by significant errors (<>).
64% resulted from hacking (+5%).
38% utilized malware (+7%).
22% involved privilege misuse (+7%).
9% occurred via physical attacks (+7%).

* Source – 2009 Verizon Data Breach Investigations Report





Systems Assurance *TRADESPACE*

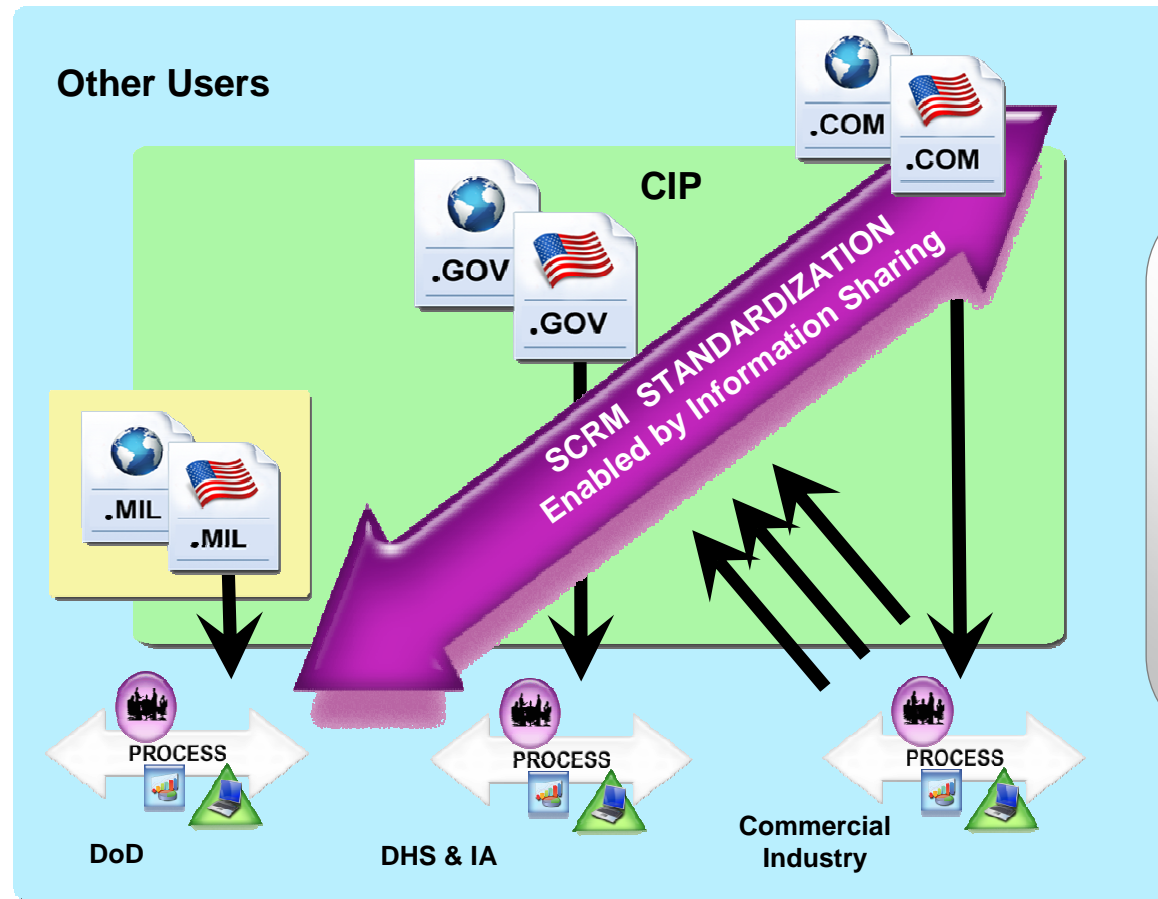




SCRM Stakeholders



US (CNCI) has vital interest in the global supply chain.



SCRM “commercially acceptable global standard(s)” must be derived from Commercial Industry Best Practices.

SCRM Standardization Requires Public-Private Collaborative Effort



CNCI-SCRM Standardization



“CNCI-SCRM is multi-pronged approach for global supply chain risk management. ...Managing this risk will require a greater awareness of the threats, vulnerabilities, and consequences associated with acquisition decisions; the development and employment of tools and resources to technically and operationally mitigate risk across the lifecycle of products (from design through retirement); the development of new acquisition policies and practices that reflect the complex global marketplace; and **partnership with industry to develop and adopt supply chain and risk management standards and best practices.**”



SCRM Standardization **Target Achievements**



In support of the US Comprehensive National Cybersecurity Initiative and Supply Chain Risk Management (CNCI-SCRM):

- **Conduct SCRM public-private outreach activities; pursue "awareness" of globalization challenges and SCRM concept.**
- **Lead SCRM Standardization activities; pursue commercially acceptable global sourcing standard(s).**

May 2011- approval of ISO requirement for ICT SCRM standard

Dec 2011- develop ISO ICT SCRM standard (for ISO staffing)

Oct 2013- publish SCRM ISO Standard



***CyberSecurity, US CNCI-SCRM,
Public-Private STANDARDIZATION ...***



Don.Davidson@osd.mil
Trusted Mission Systems & Networks
OASD-NII / DoD CIO

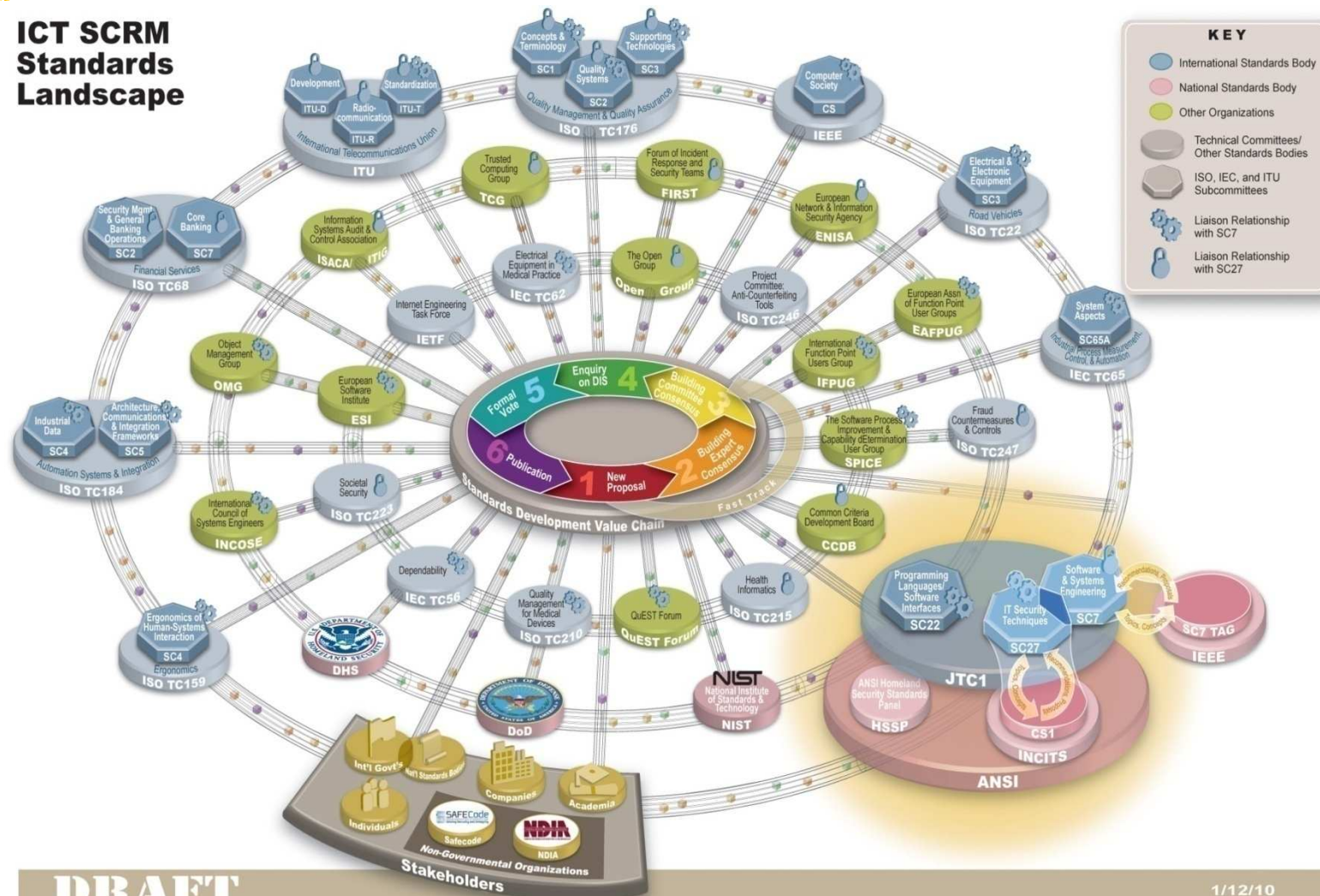


Standards Development Organizations

SDOs Landscape: an SCRMM Perspective



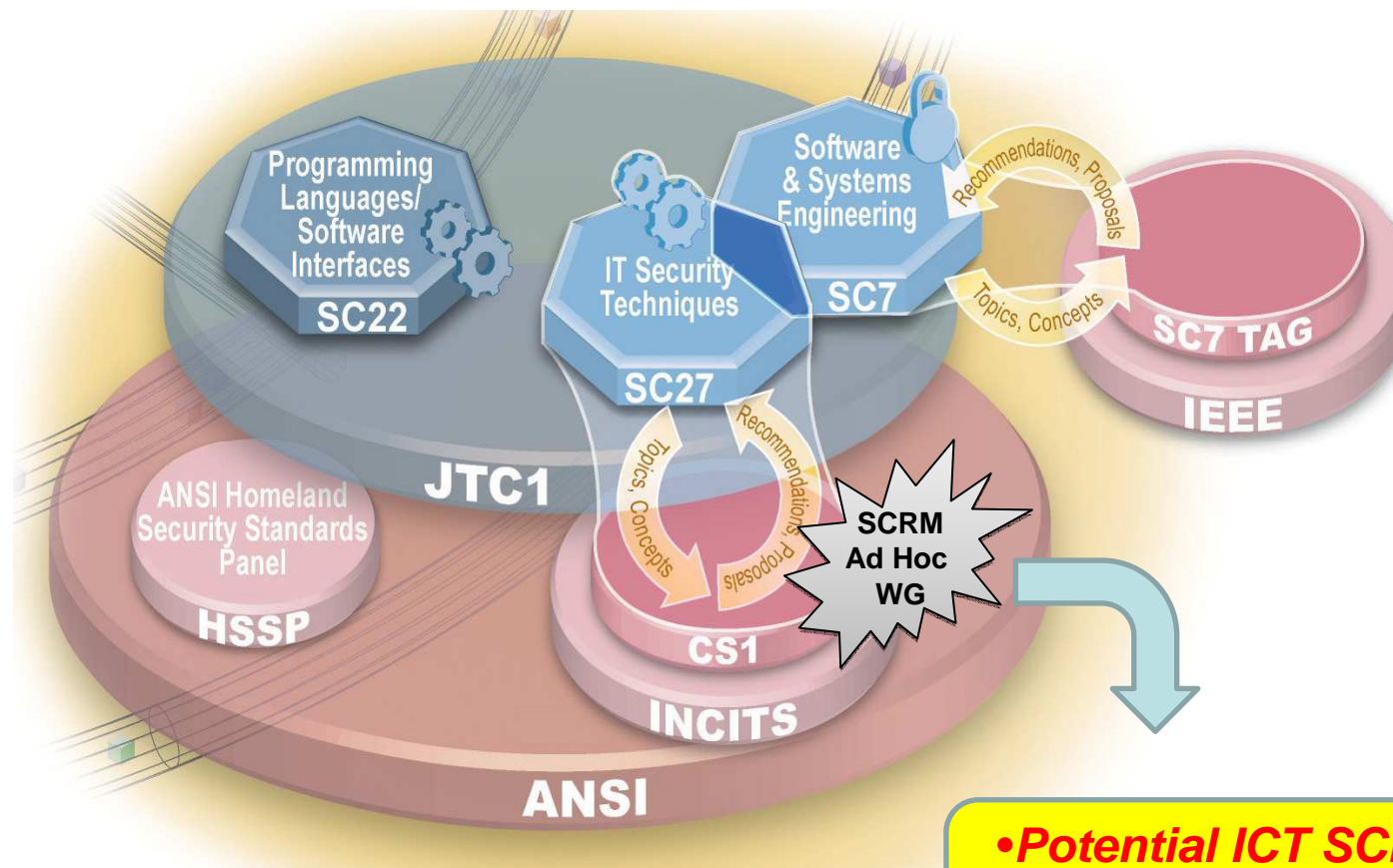
ICT SCRMM Standards Landscape





SCRM Study Periods:

Nov'09 – Apr'10 / May-Oct'10



- **Potential ICT SCRM ISO Standard**
- **Development 2010-2013**
- **Adoption 2013-2016**